WHAT IS CLAIMED IS:

1. A method of authenticating and verifying that a content file accessed by a computer is identical to the content file originally received by the computer, comprising the steps of:

registering a content file received at the computer, comprising:

generating a first digital signature of the content file, using a first key;

generating a secondary digital signature of the first digital signature and a file name of the content file, using the first key; and

storing the content file, the first digital signature, the file name, and the secondary digital signature;

accessing the stored content file, the stored first digital signature, the stored file name, and the stored secondary digital signature;

validating the first digital signature of the stored content file, using a second key corresponding to the first key; and

validating the secondary digital signature of the stored content file, using the second key.

2. A method of authenticating and verifying the integrity of a content file delivered from a server computer to a client computer over a network, comprising the steps of:

registering a content file by generating unique registration information using a first key;

storing the content file and the registration information on the server computer;

accessing the content file and the registration information in response to a request from the client computer;

authenticating the integrity of the content file and the registration information accessed by the server computer by use of a second key; and

transmitting the authenticated content file and registration information to the client computer.

3. A method of authenticating and verifying the integrity in accordance with claim 1, wherein the first key is a private key, the second key is a public key, and including the step of providing the client computer with a public key corresponding to a private key maintained by the server computer.

4. A method of authenticating and verifying the integrity of a content file in accordance with Claim 2, wherein the client computer can use the public key to generate registration information unique to the content file transmitted from the server computer and can validate the registration information generated using the public key relative to the registration information transmitted from the server computer.

5. A method of authenticating and verifying the integrity of a content file in accordance with Claim 2, wherein the step of providing the client computer with a public key comprises transmitting to the client computer a consumer application having the public key embedded therein.

6. A method of authenticating and verifying the integrity of a content file in accordance with Claim 2, wherein the step of providing the client computer with a public key comprises transmitting to the client computer a digital certificate having the public key embedded therein.

7. A method of authenticating and verifying the integrity of a content file in accordance with Claim 2, wherein the step of registering a content file by generating unique registration information comprises:

generating a server digital signature of the content file, using the private key; and

storing the server digital signature along with a file name of the content file.

8. A method of authenticating and verifying the integrity of a content file in accordance with Claim 7, wherein the step of authenticating the integrity of the content file and the registration information comprises:

validating the server digital signature accessed by the server computer, using the public key.

9. A method of authenticating and verifying the integrity of a content file in accordance with Claim 7, wherein the step of registering a content file by generating unique registration information further comprises:

generating a secondary digital signature of the server digital signature and the file name, using the private key; and

storing the secondary digital signature along with the server digital signature and the file name.

10. A method of authenticating and verifying the integrity of a content file in accordance with Claim 9, wherein the step of authenticating the integrity of the content file and the registration information comprises:

validating the secondary digital signature accessed by the server computer, using the public key.

11. A method of authenticating and verifying the integrity of a content file in accordance with Claim 10, wherein the step of authenticating the integrity of the content file and the registration information further comprises:

validating the server digital signature accessed by the server computer, using the public key.

12. A method of authenticating and verifying the integrity of content delivered over a public network in response to a request transmitted from a client computer to a server computer, comprising the steps of:

providing the client computer with a public key corresponding to a private key maintained by the server computer;

generating server registration information unique to each content file stored on the server computer, using the private key;

assembling a primary list identifying each content file responsive to the client computer's request;

transmitting to the client computer the primary list and the server registration information associated with each content file identified in the primary list;

authenticating and verifying any content files identified in the primary list which are already resident on the client computer, comprising the steps of:

assembling a matching list identifying each content file identified in the primary list which is stored on the client computer and a non-matching list identifying each content file identified in the primary list which is not stored on the client computer;

validating the server registration information received from the server computer for each content file identified in the matching list, using the public key; and

removing from the matching list and adding to the non-matching list each content file identified in the matching list for which the server registration information is not successfully validated;

transmitting to the client computer each content file identified in the non-matching list; and

validating the server registration information for each content file received from the server computer and identified in the non-matching list, using the public key.

13. A method of authenticating and verifying the integrity of content delivered over a public network in accordance with Claim 12, wherein the step of providing the client computer with a public key comprises transmitting to the client computer a consumer application having the public key embedded therein.

14. A method of authenticating and verifying the integrity of content delivered over a public network in accordance with Claim 12, wherein the step of providing the client computer with a public key comprises transmitting to the client computer a digital certificate having the public key embedded therein.

15. A method of authenticating and verifying the integrity of a content file in accordance with Claim 12, wherein the step of generating server registration information unique to each content file comprises:

generating a server digital signature of each content file, using the private key; and

storing the server digital signature along with a corresponding file name for each content file.

16. A method of authenticating and verifying the integrity of a content file in accordance with Claim 15, wherein, prior to the step of transmitting to the client computer the primary list and the server registration information associated with each content file identified in the primary list, the method further comprises the step of:

validating the server digital signature of each content file identified in the primary list and stored on the server computer, using the public key.

17. A method of authenticating and verifying the integrity of a content file in accordance with Claim 15, wherein the step of generating server registration information unique to each content file further comprises

generating a secondary digital signature of each server digital signature and each corresponding file name, using the private key; and

storing each secondary digital signature along with the corresponding server digital signature and file name.

18. A method of authenticating and verifying the integrity of a content file in accordance with Claim 17, wherein, prior to the step of transmitting to the client computer the primary list and the server registration information associated with each content file identified in the primary list, the method further comprises the step of:

authenticating the integrity of each content file identified in the primary list and stored on the server computer, comprising the steps of:

validating the server digital signature of each content file identified in the primary list and stored on the server computer, using the public key; and

validating the secondary digital signature of each content file identified in the primary list and stored on the server computer, using the public key.

19. A method of browsing the web by requesting content from a server computer over a public network and displaying the content to a user on a client computer only after the integrity of such content has been authenticated and verified, comprising the steps of:

transmitting a request to the server computer for content necessary to build a displayable web page;

receiving from the server computer a primary list identifying each file necessary to build the web page and a server digital signature uniquely associated with each file identified in the primary list;

validating the server digital signature for each file stored locally on the client computer which is identified in the primary list;

transmitting to the server computer a secondary list identifying each file identified in the primary list which is not stored locally on the client computer or for which the server digital signature is not successfully validated;

receiving from the server computer each file identified in the secondary list;

validating the server digital signature for each file received from the server computer and identified in the secondary list; and

if the server digital signature for each file is validated, displaying on the client computer a web page incorporating the content of each file identified in the primary list if the server digital signature is successfully validated for every file received from the server computer and identified in the secondary list.

20. A method of browsing the web in accordance with Claim 19, further comprising the step of:

deleting each file stored locally on the client computer for which the server digital signature is not successfully validated.

21. A method of browsing the web in accordance with Claim 19, further comprising the step of:

displaying on the client computer an error message if the server digital signature is not successfully validated for any file received from the server computer and identified in the secondary list.

22. A method of browsing the web in accordance with Claim 20, further comprising the step of:

transmitting to the server computer an error list identifying each file identified in the secondary list for which the server digital signature is not successfully validated.

23. A method of browsing the web in accordance with Claim 22, further comprising the steps of:

receiving from the server computer each file identified in the error list;

validating the server digital signature for each file received from the server computer and identified in the error list; and

displaying on the client computer a web page incorporating the content of each file identified in the primary list if the server digital signature is successfully validated for every file received from the server computer and identified in the error list.

24. A web content delivery system for delivering web content from a server computer to a client computer over a public network and displaying the content on the client computer only after the integrity of such content has been authenticated and verified, comprising the steps of:

providing the client computer with a public key which corresponds to a private key maintained at the server computer;

generating at the server computer cryptographic registration information for each content file stored on the server computer, comprising the steps of:

generating a server digital signature of each content file stored on the server computer, using the private key;

generating a secondary digital signature of each server digital signature and corresponding file name, using the private key; and

storing on the server computer each file name along with the corresponding server digital signature and secondary digital signature;

transmitting from the client computer to the server computer a request for content necessary to build a displayable web page;

assembling at the server computer a primary list identifying each content file responsive to the request for content;

authenticating and verifying any content files identified in the primary list which are stored on the server computer, comprising the steps of:

validating the server digital signature of each content file identified in the primary list, using the private key; and

validating the secondary digital signature of each content file identified in the primary list;

transmitting from the server computer to the client computer the primary list and the server digital signature of each content file identified in the primary list;

authenticating and verifying any content files identified in the primary list which are already resident on the client computer, comprising the steps of:

assembling a matching list identifying each content file identified in the primary list which is stored on the client computer and a non-matching

list identifying each content file identified in the primary list which is not stored on the client computer;

validating the server digital signature of each content file stored on the client computer and identified in the matching list, using the public key; and

removing from the matching list and adding to the non-matching list each content file identified in the matching list for which the server digital signature is not successfully validated;

transmitting from the server computer to the client computer each content file identified in the non-matching list; and

validating the server digital signature of each content file received from the server computer and identified in the non-matching list, using the public key.

25. A system for verification of file content which is transmitted from a server to a client through a network, comprising:

said server having therein a server program for:

(a) registering a plurality of files which comprise said content by producing registration information which includes a digital signature for each said file by use of a private key, and

(b) storing said files and said registration information,

(c) sending a list said files and said registration information to said client when said file content is requested, and

(d) sending the ones of said files requested by said client to said client via said network,

said client of said server having therein a client program for:

(a) requesting said file content via said network,

(b) upon receiving said list of said files and said registration information , detecting the presence of any of said files on said list in local storage for said client,

(c) for said local files, which are on said list and located in said local storage, verifying said local files by use of said registration information, and

(d) requesting from said server the ones of said files on said list which were not verified by said client.

26. An article of manufacture comprising a computer program carrier readable by a computer and embodying one or more instructions executable by the computer to perform steps for authenticating and verifying that a content file accessed by a server computer is identical to the content file originally received by the server computer, comprising:

registering a content file received at the computer, comprising:

generating a first digital signature of the content file, using a first key;

generating a secondary digital signature of the first digital signature and a file name of the content file, using the first key; and

storing the content file, the first digital signature, the file name, and the secondary digital signature;

accessing the stored content file, the stored first digital signature, the stored file name, and the stored secondary digital signature;

validating the first digital signature of the stored content file, using a second key corresponding to the first key; and

validating the secondary digital signature of the stored content file, using the second key.

27. An article of manufacture comprising a computer program carrier readable by a computer and embodying one or more instructions executable by the computer to perform steps for authenticating and verifying the integrity of a content file delivered from a server computer to a client computer over a network, comprising:

registering a content file by generating unique registration information using a first key;

storing the content file and the registration information on the server computer;

accessing the content file and the registration information in response to a request from the client computer;

authenticating the integrity of the content file and the registration information accessed by the server computer by use of a second key; and

transmitting the authenticated content file and registration information to the client computer.

28. An article of manufacture comprising a computer program carrier readable by a computer and embodying one or more instructions executable by the computer to perform steps for browsing the web by requesting content from a server computer over a public network and displaying the content to a user on a client computer only after the integrity of such content has been authenticated and verified, comprising:

transmitting a request to the server computer for content necessary to build a displayable web page;

receiving from the server computer a primary list identifying each file necessary to build the web page and a server digital signature uniquely associated with each file identified in the primary list;

validating the server digital signature for each file stored locally on the client computer which is identified in the primary list;

transmitting to the server computer a secondary list identifying each file identified in the primary list which is not stored locally on the client computer or for which the server digital signature is not successfully validated;

receiving from the server computer each file identified in the secondary list;

validating the server digital signature for each file received from the server computer and identified in the secondary list; and

if the server digital signature for each file is validated, displaying on the client computer a web page incorporating the content of each file identified in the primary list if the server digital signature is successfully validated for every file received from the server computer and identified in the secondary list.

29. An apparatus for authenticating and verifying a content file, comprising:

a computer in a computer network; and

one or more computer programs, performed by the computer, for registering a content file received at the computer, comprising:

generating a first digital signature of the content file, using a first key;

generating a secondary digital signature of the first digital signature and a file name of the content file, using the first key; and

storing the content file, the first digital signature, the file name, and the secondary digital signature;

accessing the stored content file, the stored first digital signature, the stored file name, and the stored secondary digital signature;

validating the first digital signature of the stored content file, using a second key corresponding to the first key; and

validating the secondary digital signature of the stored content file, using the second key.

30. An apparatus for authenticating and verifying integrity of a content file, comprising:

a server computer in a computer network;

a client computer connected to the server computer via the computer network; and

one or more computer programs, performed by the server computer, for:

registering a content file by generating unique registration information using a first key;

storing the content file and the registration information on the server computer;

accessing the content file and the registration information in response to a request from the client computer;

authenticating the integrity of the content file and the registration information accessed by the server computer by use of a second key; and

transmitting the authenticated content file and registration information to the client computer.

31. An apparatus for browsing the web by requesting content from a server computer over a public network and displaying the content to a user on a client computer only after the integrity of such content has been authenticated and verified, comprising, comprising:

a server computer in a computer network;

a client computer connected to the server computer via the computer network; and

one or more computer programs, performed by the client computer, for:

transmitting a request to the server computer for content necessary to build a displayable web page;

receiving from the server computer a primary list identifying each file necessary to build the web page and a server digital signature uniquely associated with each file identified in the primary list;

validating the server digital signature for each file stored locally on the client computer which is identified in the primary list;

transmitting to the server computer a secondary list identifying each file identified in the primary list which is not stored locally on the client computer or for which the server digital signature is not successfully validated;

receiving from the server computer each file identified in the secondary list;

validating the server digital signature for each file received from the server computer and identified in the secondary list; and

if the server digital signature for each file is validated, displaying on the client computer a web page incorporating the content of each file identified in the primary list if the server digital signature is successfully validated for every file received from the server computer and identified in the secondary list.